UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,791	10/30/2001	Randal W. Glass	IRID-0479	1214

7590 08/26/2004

Susan C. Murphy, Esquire
WOODCOCK WASHBURN LLP
46th Floor
One Liberty Place
Philadelphia, PA 19103

EXAMINER	
STULBERGER, CAS P	

ART UNIT	PAPER NUMBER
2132	12

DATE MAILED: 08/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/020,791	GLASS, RANDAL W.	
	Examiner	Art Unit	
	Cas Stulberger	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *3 and 20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 10/30/2001; amendment filed 5/28/2004.

2. Claims 1-20 are pending in the case. Claim 3 and 20 are cancelled. Claims 1, 11, 14, and 17 are independent claims.

Response to Amendment

3. Applicant's arguments, see ammendment C, filed 5/28/2004, with respect to the rejection(s)of claim(s) 1-20 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,167,517 to Gilchrist et al in view of U.S. Patent No. 6,202,151 B1 to Musgrave have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of U.S. Patent No. 6,076,167 to Borza.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 7, and 9, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,167,517 to Gilchrist et al in view of U.S. Patent No. 6,202,151 B1 to Musgrave et al. and in further view of U.S. Patent No. 6,076,167 to Borza.

In regards to claim 1-2, Gilchrist discloses that a biometric authentication system receives a biometric input and compares it against a prerecorded template containing biometric data associated with the user to determine whether to grant the user access to a service on the host system (Gilchrist: column 1, lines 42-47). This meets the limitation of "a sensor to collect biometric data, and a biometric template generator, coupled to the sensor, to convert the biometric data into a biometric template." Gilchrist also discloses that the client computing system contains a secure encryption key in order to guard against malicious users on the client system (Gilchrist: Abstract). However Gilchrist does not disclose "signing the biometric data with a signature corresponding to the sensor."

Musgrave discloses creating a digital signature by encrypting a hashed value with a private key (Musgrave: column 2, lines 23-25). Musgrave also discloses that private keys are physically stored on computers and/or electronic storage devices, and such private keys are not limited to actual human individuals (Musgrave: column 2, lines 34-46). This meets the limitation of "signing the biometric data with a signature corresponding to the sensor."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of encrypting data with an encryption key as disclosed by Gilchrist with the method of using the private key to encrypt data to generate a digital signature as disclosed by Musgrave in order to provide greater integrity, privacy, and a degree of authentication (Musgrave: column 1, lines 61-62).

However Gilchrist does not disclose "an encryptor coupled to the security code generator to encrypt the signed biometric data." Borza discloses encrypting the biometric information with the public key received from the server and transmitting the now encrypted biometric data to the

server (Borza: column 6, lines 54-59). This meets the limitation of "encrypting the signed data package using the server public key."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of signing biometric data as disclosed by Gilchrist with the method of encrypting the biometric data with a server public key as disclosed by Borza in order to provide a secure communication channel (Borza: column 1, lines 25-41).

In regards to claim 7, Gilchrist discloses that the biometric sample taken from the user I compared with the biometric template to produce a comparison result (Gilchrist: column 2, lines 31-33). This meets the limitation of "further comprising a biometric matcher to compare a two biometric templates to determine whether the two biometric templates match and to generate a match result."

In regards to claim 9, Gilchrist discloses that a way to prevent templates or biometric samples from being tampered with when transferred across a network is to encrypt the templates or samples (Gilchrist: column 2, lines 7-9). This meets the limitation of "further comprising a security module to decrypt and validate a previously enrolled biometric template received via the network."

6. Claims 4-6, 8, 10-13, 17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,167,517 to Gilchrist et al in view of U.S. Patent No. 6,202,151 B1 to Musgrave et al. and in further view of U.S. Patent No. 6,076,167 to Borza as

applied to claims 1-2, 7, and 9 above, in view of U.S. Patent No. 6,310,966 B1 to Dutude et al. and further in view of U.S. Patent no 5,280,527 to Gullman et al.

In regards to claims 4-6, 8, 10-13, 17, and 20, Gilchrist discloses a method for authenticating the identity of a user in order to secure access to a host system. The host receives an identifier for the user from the client. The host retrieves a template containing biometric data associated with the user and the template is returned to the client. The client then gathers a biometric sample from the user and compares the sample with the template producing a comparison result (Gilchrist: column 2, lines 25-33). This meets the limitation of "obtaining a biometric sample at the imaging device." The client then computes a message digest using the template, the comparison result, and an encryption key, and sends the message digest to the host system. The host system receives the message digest and authenticates the user by determining whether the message digest was computed using the template, the encryption key, and a comparison result indicating a successful match between the biometric sample and the template. If so, the host has confidence that the client has successfully matched the template with the biometric sample, and the client is allowed to access a service on the host system (Gilchrist: column 2, lines 34-48). This meets the limitations of "generating a data package comprising the biometric sample, and transmitting the data package to the server, receiving the data package at the server, and authenticating the imaging device at the server." Gilchrist however does not disclose "signing the biometric sample at the imaging device, generating a data package comprising a token, the signature, and an imaging device public key certificate, and validating the signature and the token at the server."

Dulude discloses biometric identification is combined with digital certificates for electronic authentication as biometric certificates (Dulude: Abstract, first sentence). A hash valued of the biometric data and the transaction first data, which includes the user id data identifying the first user and associating the first user with the remainder of the transaction first data, is created (Dulude: column 5, lines 59-62; column 6, lines 1-5). The hashed value is then sent to a digital signature function, in which the hashed value is signed; that is, encrypted using the private key of the first user to generate a digital signature incorporating the first hash value. The signature is then sent to the network (Dulude: column 6, lines 13- 17). This meets the limitation of "generating a data package comprising the signature, and an imaging device public key certificate." The biometric certificate is received and decrypted by the certifying authority using the public key of the certifying authority (Dulude: column 6, lines 60-62). The first hash value is then extracted (Dulude: column 7, lines 1-3). The receiving section authenticates the first hash value by attempting to recreate the first has value using a second hash function, identical to the first has function of the transmitting section. The hash values are then compared to determine a match between the first and second hash values. A validation signal is generated to indicate whether or not both independently generated hash values match (Dulude: column 7, lines 4-19). This meets the limitation of "validating the signature at the server."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method for authenticating the identity of a user in order to secure access to a host system as disclosed by Gilchrist et al. with the method of combining digital certificates with biometric information in order to create biometric certificates as

disclosed by Dulude et al. in order to provide for increased security and accuracy (Dulude: column 3, lines 27-30).

Neither Gilchrist nor Dulude however teach generating a token. Gullman discloses a security apparatus which receives a biometric input from a user. The user in put is then compared to a template to determine a correlation factor. The correlation factor, a fixed code, and either a time-varying code or a challenge code then is combined to generate a token. The token is then displayed to the user, who then enters the token at an access device. The token is forwarded to the host, which processes the token to determine whether access is permitted (Gullman: Abstract).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method for authenticating the identity of a user in order to secure access to a host system as disclosed by Gilchrist et al. with the method for generating a token as disclosed by Gullman in order to provide security measures for safeguarding access to information (Gullman: column 1, lines 14-18).

7. Claims 14, 15, 16, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,167,517 to Gilchrist et al in view of U.S. Patent No. 6,202,151 B1 to Musgrave et al. and in further view of U.S. Patent No. 6,076,167 to Borza in view of U.S. Patent No. 6,310,966 B1 to Dutude et al. and further in view of U.S. Patent No. 5,280,527 to Gullman et al applied to claims 1-2, 4-13, 17, and 20 above, and further in view of U.S. Patent No. 6,092,201 to Turnbull et al.

Gilchrist however does not disclose "transmitting the public key from the imaging device to a certification authority; generating an imaging device public key certificate at the certification authority; generating a certification authority public key certificate at the certification authority; and transmitting the imaging device public key certificate and the certification authority public key certificate to the imaging device." Turnbull discloses that to ensure that the receiving party is using an authentic signature verification public key of the sending party, it utilizes the sending party's signature public key certificate, obtained from the sending party itself, from a directory, from a certification authority, or from any other available source (Turnbull: column 1, lines 64-67; column 2, lines 1-2). This meets the limitation of "generating an imaging device public key certificate at the certification authority." Turnbull also discloses the signature public key certificate includes the public key of the sending party and a signature of a certification authority. The receiving party using a trusted public key of the certification authority verifies the signature of the certification authority on this certificate (Turnbull: column 2, lines 2-7). This meets the limitation of "generating a certification authority public key certificate at the certification authority; and transmitting the imaging device public key certificate and the certification authority public key certificate to the imaging device."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of for authenticating the identity of a user in order to secure access to a host system as disclosed by Gilchrist et al. with the method of transmitting a public key certificate to the user in order to extend secure communication operations by obtaining trustworthy certificates from end-users that maintain a shared list (Turnbull: column 2, lines 60-62).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (703) 305-8034None. The examiner can normally be reached on Monday - Friday, 9:00A.M. - 5:00P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications, (703) 746-7240 for drafts, and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CS

CS
August 20, 2004

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100